Blockaid

Blockaid's View on Security

A comprehensive look at onchain risk, why legacy security models fall short, and how Blockaid protects the newest generation of financial infrastructure.

Blockaid

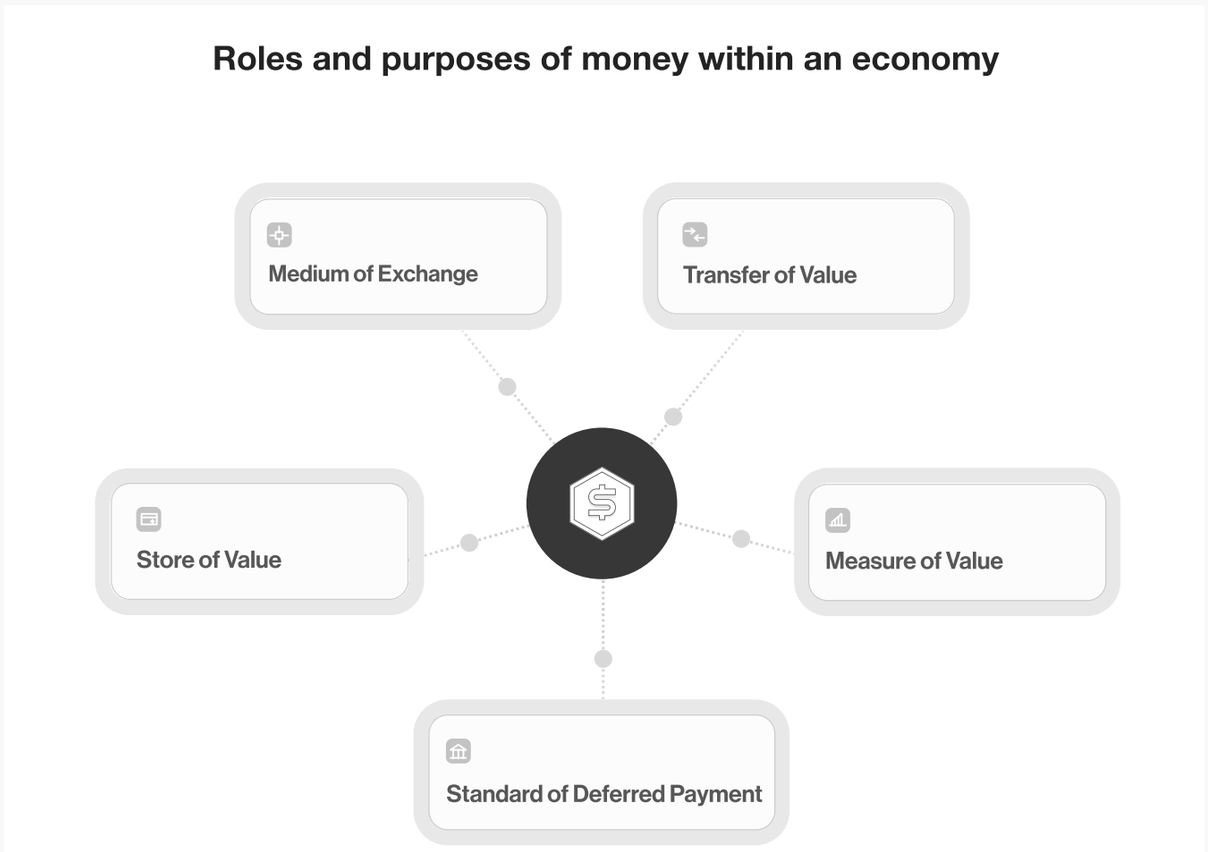
CONTEXT

Theft Is as Old as Humanity — Technology Just Makes It Easier

For as long as humans have created, traded, settled, and stored value, there have been those who exploit trust in that system of "money".

Theft prevention is continuously challenged by the changing functions of money: its method and speed of exchange, its unit of account, and its accepted forms.

Technology has always evolved money and crime. Each major evolution has come with new vulnerabilities that attract new methods of crime.



Time period	Tech evolution	Money evolution	Crime evolution
1910s-20s	GM & Sears introduce mass market automobiles & appliances, available on credit	Destigmatization of buying on credit	Forgery, Ponzi schemes, predatory lending, money laundering
1950s-70s	Diners Club and Bank of America introduce multipurpose charge cards and revolving credit	Plastic credit cards become an accepted form of payment	Credit card theft, card skimming, impersonation
1990s-2000s	PayPal introduces person-to-person transfers via email	Physical cash or card are not longer needed in a world of e-commerce and online banking	Email phishing, identity theft, password harvesting, ransomware
2008+	iPhones and social media apps drive 24/7/365 global connectivity	Faster, higher volume, 100% digital payments	Mass data breaches, social engineering scams
2010s+	Bitcoin introduced decentralized, programmable, self-custodial money	Tokenized assets, DeFi protocols	Wallet drainers, rugpulls, smart contract exploits
2025+	AI + open banking APIs	Agentic payments	Deepfakes, synthetic identity theft

Blockaid

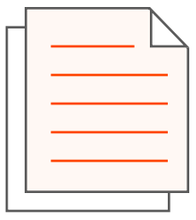
CONTEXT

Web3 Security: How We Got Here

To understand onchain security, it helps to define the three eras of the internet:

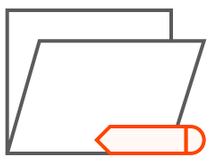
Web 1 - Read Only

Users consumed information but did not participate. The attack surface was relatively narrow — primarily targeting infrastructure and content.



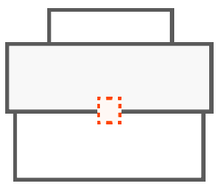
Web 2 - Read & Write

The explosion of digital commerce, social networks, and cloud-based financial services brought credential theft, phishing, account takeover, identity theft, payment fraud, and more.



Web 3 - Ownership

For the first time, users hold their own assets online — without the intermediaries, custodians, or safety nets that traditional financial infrastructure provides.



Web3's ownership model is transformative.
But it also makes security an acute challenge.

Blockaid

THE CHALLENGE

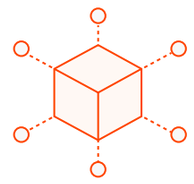
Why Onchain Is Different

Blockchains come with structural properties that are features and risks simultaneously:

01

Networks are public

Every transaction, wallet balance, and smart contract interaction is visible to anyone. Attackers can conduct reconnaissance without ever penetrating a target network.



02

Trust is codified in composable infrastructure

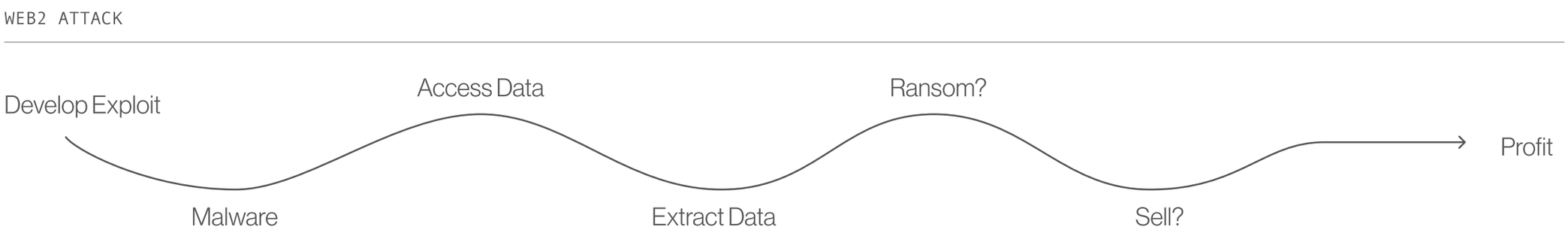
Intermediaries are replaced by cryptography, open-source code, and consensus mechanisms. Every dependency creates a new surface for manipulation.

03

Attacker time to value is extremely short

In web3, the window to extract funds can be measured in minutes and seconds. Prevention is not merely preferable to detection — it is essential.

Attacker time to value



The security models that worked in the Web 2 era are insufficient for our increasingly onchain world. Real-time detection and prevention is not a nice-to-have. It is the baseline.

Blockaid

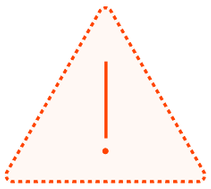
THE CHALLENGE

Three Categories of Onchain Risk

Onchain risk spans three interconnected domains. Treating them as silos is, in itself, a vulnerability.

Cyber Risk

Theft from exploits targeting vulnerabilities in smart contracts or dependent onchain infrastructure to drain funds. Compromise of private keys, dApp DNS, or unchecked transaction calls. $2.58B stolen through web3 vulnerabilities in 2025 alone.



Fraud Risk

First-party fraud, third-party fraud, merchant fraud, and incentive abuse. Sophisticated social engineering schemes originating in Web 2 routinely funnel victims toward Web3 endpoints where funds are extracted.

Compliance Risk

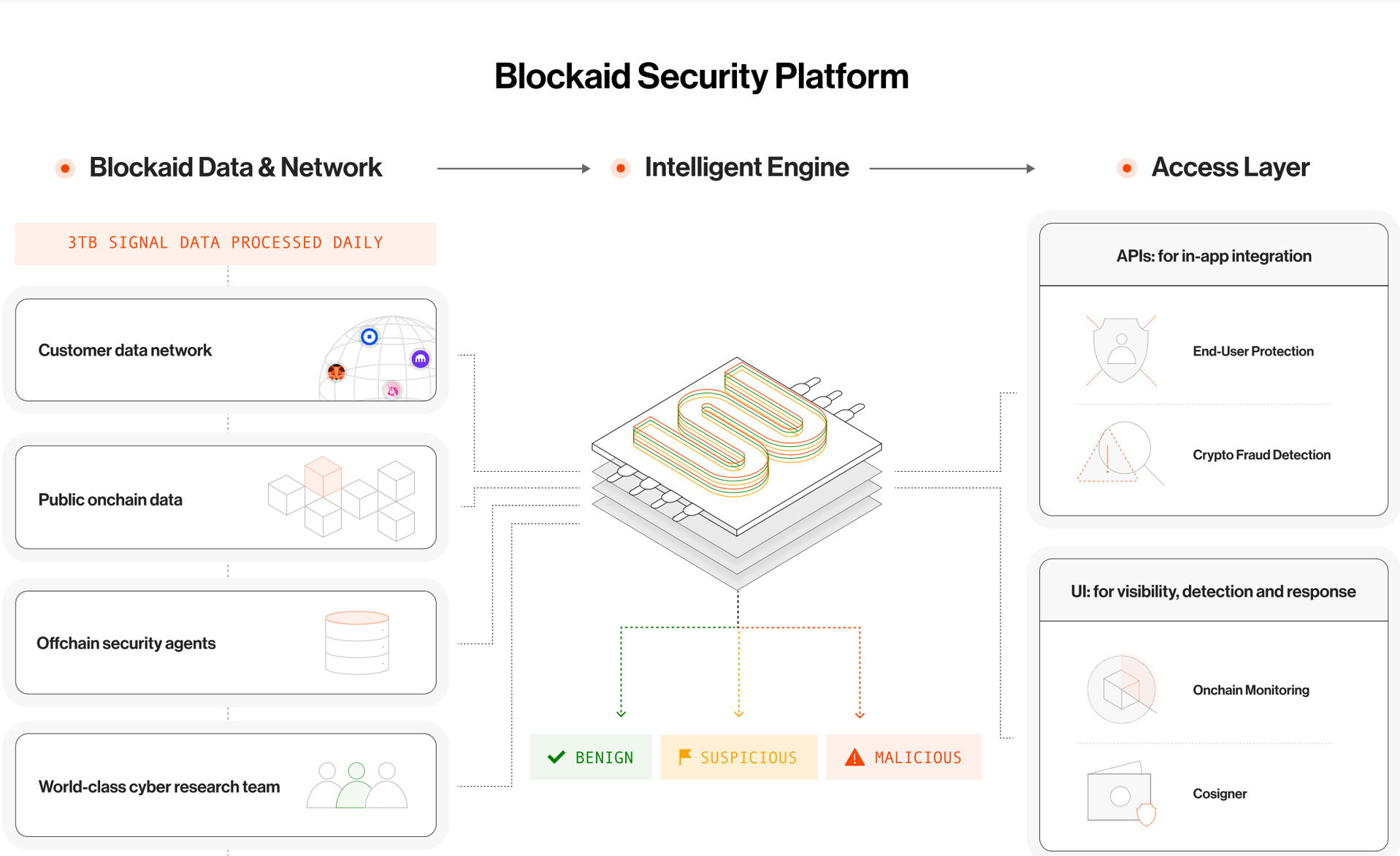
Anti-money laundering, sanctions screening, illicit fund flows, and regulatory exposure. As stablecoins become mainstream settlement infrastructure, compliance is a first-order concern — not an afterthought.

These three risk types are not independent. A threat actor that exploits a smart contract vulnerability immediately moves to laundering the funds onchain. Fraud schemes — particularly money muling — are a common method to disguise stolen funds and can be spun up quickly.

THE SOLUTION

A Single Platform for Real-Time Security, Fraud & Compliance

Blockaid was built around a fundamental conviction: that onchain risk assessments must operate in real time, across the full stack of signals — onchain, online, behavioral, and social.



Platform Foundation

Blockaid's capabilities are built on detection primitives continuously enriched by over 3TB of signals, daily. Our intelligent detection engine determines threats in <300 ms and with supporting evidence.

Blockaid

THE SOLUTION

Core Scanning Capabilities

Transaction Scanning

Simulates and validates a transaction, and all its parameters, before signing. This surfaces approvals, fund movements, and contract interactions.

dApp Scanning

Analyzes web3 frontend apps for signs of compromise, malicious code injection, or fraudulent behavior the moment a wallet connects.

Chain Scanning

Behavioral & address exposure analyses across smart contracts, chains, bridges & oracles

Compliance Scanning

Evaluates crypto addresses for 24+ exposure categories, automatically tagging illict / sanctioned funds in real-time to prevent fund laundering

Token Scanning

Continuously reads metadata on 40M+ tokens to identify rugpulls, honeypots, and spam campaigns — before users interact with them.

These scanning capabilities are complemented by internet-wide security agents that gather and test web2 surfaces including: DNS registrations, ad networks, phishing domains, social media, and Telegram channels — connecting offchain and onchain threat environments.

By integrating with the most widely used wallets and exchanges, Blockaid screens 500M+ transactions every month. This proprietary behavioral data creates an intelligence flywheel: every transaction simulated strengthens detection for all customers.

WHY BLOCKAID

Blockaid by the Numbers

TRANSACTIONS SCANNED	DAPP INTERACTIONS ANALYZED	ASSETS SECURED
6B+	3B+	$325B+

Note: cumulative data since 2022

THE STAKES

Why This Matters Now

The onchain security problem is not a niche concern for crypto insiders. It is a foundational challenge for the next phase of global financial infrastructure.

Major financial institutions — J.P. Morgan, Fidelity, UBS, and others — are scaling their blockchain initiatives. Stablecoins are increasingly used for cross-border payments, remittances, and institutional settlement. The U.S. government has begun setting standards to foster adoption while mitigating risk.

As the value flowing through onchain systems grows, so does the incentive to attack them. Protecting that value — and the trust of the users, institutions, and regulators whose confidence underpins the entire ecosystem — requires security infrastructure that is real-time, comprehensive, and purpose-built.

Blockaid

Conclusion

Theft has always followed value. The shift to onchain technology has not changed that dynamic — it has intensified it and expanded the surface areas available to attackers. Risk is no longer separated by cyber, compliance, and fraud as all dimensions can take place simultaneously.

Meeting this challenge requires moving beyond the reactive, siloed security approaches of the past. It requires a platform that sees across every relevant signal — onchain and offchain, behavioral and social — and that operates at the speed of the blockchain itself.

Blockaid's mission is to make onchain operations trustworthy at scale: for the wallets and protocols that power the ecosystem today, and for the institutions and billions of users who will depend on it tomorrow.

◆ TRUSTED BY

coinbase · METAMASK · world · Revolut · Polymarket

Uniswap · Stellar · Fireblocks · Sui · zerion

rainbow · OpenSea · STARKNET · LEDGER · ...and hundreds more

◆ GET IN TOUCH

@blockaid_ · @blockaid · https://blockaid.io/